Internet Intelligence and Investigation Policy (Surrey and Sussex) (1155/2024)

Abstract

This policy provides instruction and guidance to Surrey Police and Sussex Police staff for their professional use of the internet to review and extract information for the purpose of intelligence gathering or to be used in evidence.

Policy

1. Introduction

1.1 This policy applies to all police personnel researching the internet for investigative or intelligence purposes and ensures a professional, lawful, and ethical approach to Internet Intelligence and Investigations. The internet, and in particular social media platforms, are a rich and cost-effective source of intelligence and information which can be of significant evidential value. This policy actively encourages police personnel to make use of the internet when conducting their enquiries, whenever it is appropriate for them to do so. Internet Intelligence and Investigation is abbreviated in this document as III, but is also commonly abbreviated as 3i, triple(i), OSINT and open source. This policy is now administered by the Digital Investigation Support Unit (DISU) established in 2022 and has been re-written to reflect the changes in capability within internet, intelligence, and investigation (III). For guidance, please visit Digital Investigation Support Unit (DISU).

2. Scope

2.1 This policy covers the use of the internet for all investigation and intelligence purposes. It does not cover the use of the internet as an engagement tool or Undercover Online (UCOL), however, can be used as a guiding influence to provide understanding of available training and equipment requirements to engage in such activity. This policy does not cover acceptable use of the internet and social media (instead see Surrey Police and Sussex Police Information Security Policy (722) "Use of Internet Procedure" and Social Media Policy (Surrey and Sussex) (1086).

2.2 In addition, this policy does not cover ‘account takeovers’ where members of the public have provided their account details to law enforcement to access information with consent. Instead, this police concerns itself with police employees accessing the internet overtly and covertly to extract information.

3. Policy Statement

3.1 Surrey Police and Sussex Police will ensure that access and use of the internet for intelligence or investigative purpose is carried out professionally, lawfully, and ethically.

3.2 Police personnel researching the internet for policing purposes will be appropriately trained and have a good working knowledge of the potential of the internet as a source, and the knowledge to conduct internet enquiries.

3.3 Law Enforcement Agencies must comply with all relevant legislation including that relating to the surveillance of individuals, which applies equally to the internet as to the physical environment.

3.4 Any investigations or intelligence gathering conducted using the internet must be carried out in accordance with the legal, ethical and moral obligations placed on public authorities by the European Convention on Human Rights (ECHR), most notably Article 8 (respect for private and family life); does not place the Organisation at risk of legal challenge, or place individuals involved in research avoidable personal risk / vulnerability from their online activities. Further to this, activities must not jeopardise any ongoing or future investigations or law enforcement activities. This policy ensures we meet these requirements whilst still maintaining a critical avenue for investigation.

Procedure

1. Responsibilities

1.1 Practitioner Role:

• Safe research using the internet to enhance criminal investigations;

• Lawful Capture of Evidence / Intelligence;

• Dissemination of findings and material.

Responsibility:

• Complete any supervisor directed training and ensure Continual Professional Development (CPD) is current;

• Comply with relevant policies and legislation;

• Keep accurate records regarding online activity;

• Ensure, where required, information and intelligence are captured in a form that can be evidenced;

• Be able to present findings to Court or tribunal and account for actions;

• Use online profiles (hereafter referred to simply as profiles) that have been created for the investigation / task;

• Manage any profile in use to ensure that they are kept ‘live’;

• Ensure any relevant authorities are in place prior to activity when required;

• Covert III practitioners only – create covert III profiles and register with Divisional or Force Intelligence Bureau (FIB) Senior Analysts. (DISU and Anti-Corruption Unit (ACU) profiles will be managed internally within these departments).

1.2 Manager / Supervisor Role:

• Manage the online activity of team members involved in III activity;

• Manage use of profiles by team members;

• Equip their unit with relevant equipment.

Responsibility:

• Ensure team members are trained to correct level for their role prior to activity;

• Dedicate CPD and learning time to team members;

• Authorise new profile use (for Covert III) or new overt profile (for Overt III);

• Ensure covert profiles used within investigations are logged with Divisional or FIB Senior Analysts (DISU profiles will be managed by DISU and ACU profiles by ACU);

• Supervise the use of covert profiles within the investigation to ensure transparency and accountability of the use;

• Ensure any relevant authorities are in place, when required, prior to surveillance activity being conducted;

• Ensure all team members have access to relevant equipment;

• Update, or delegate to trained team members, all relevant equipment (i.e. antivirus / screen capture software / auditing software / devices / application access).

1.3 Senior Analyst Role:

• Management, de-confliction, and logging of covert profiles in central repository;

• Provide advice on internet intelligence opportunities.

Responsibility:

• Ensure all details of profiles submitted by staff are logged within the central repository (except DISU and ACU profiles);

• Ensure RIPCOM (RIPA Compliance Unit) / CAB (Central Authorities Bureau) and Professional Standards Department (PSD) have access to the repository;

• Monitor and update practice guides when required;

• Keep up to date with and share national guidance;

• Liaise with regional leads and DISU regarding good practice and developments.

1.4 Learning and Development Role:

• Provision of training materials and delivery thereof to enable practitioners and managers to fulfil role and responsibilities outlined.

Responsibility:

• Align course content and delivery with College of Policing (CoP) learning standard and skills matrix;

• Ensure sufficient access and provision to training is in place (in house or through external providers) at each of the three levels of III (core, overt and covert);

• Ensure Overt III and Covert III training is only delivered to those working in a role which necessitates such.

1.5 Corporate Communications Role:

• No specific role, in previous versions Corporate Communications have created overt profiles – this need has since become redundant as further explained in section 4.

Responsibility:

• None.

1.6 ICT Role:

• Provision of infrastructure, networks, applications, and devices that enable practitioners to carry out III activity as relevant and necessary for their role. (Note this does not include provision of non-standard and non-networked assets such as phones and sim cards).

Responsibility:

• To ensure that all equipment used for III meets and is maintained or replaced to the required standard as per the National Police Chiefs' Council (NPCC) III strategy and this policy;

• To make sufficient equipment available for III requirements;

• To enable internet use and applications for III in compliance with this policy.

1.7 RIPCOM Role:

• Advice regarding authorities and their application to III activity.

Responsibility:

• Maintaining a central record of surveillance activity as per Codes of Practice;

• Acting as a central point of reference for Regulation of Investigatory Powers Act 2000 (RIPA) related enquiries including link to Investigatory Powers Commissioners Office (IPCO);

• Ensuring quality assurance of directed surveillance applications, reviews, renewals, and cancellations;

• Developing / updating covert policy and procedures;

• Identifying / delivering training in respect of surveillance activity;

• Developing / maintaining any internal RIPCOM specific guidance on internal communications pages / sites.

1.8 DISU Role:

• Provide advanced III capability for the Surrey Police and Sussex Police predominantly operating in covert internet investigations within closed spaces along with developing best practice and guidance for III.

Responsibility:

• As practitioner and manager responsibilities above and in addition:

• (Redacted text) maintaining more realistic and robust profiles (limited to covert investigations not UCOL);

• Test new social media platforms and develop best practice for III exploitation and research;

• Test and develop processes around new technologies to make best use of III;

• Support intelligence units with capacity issues with regards III requirements;

• Maintain online tutorials, user guides and discussions for Surrey Police and Sussex Police and represent at regional and national law enforcement III groups; (See DISU – Home)

• Primary first point of contact for dark web (non-indexed web) investigation or tasking;

• Maintain this policy and procedure.

2 Why is this important?

2.1 Any activity on the internet leaves a ‘footprint’ or trace. This footprint can be investigated by individuals who find it or may well be subject to analytical algorithms which seek to determine information about the individual leaving the footprint. It is vital that any individual using the internet understands the footprint they are leaving and understands the risk around it. This risk should not be underestimated. While at first glance an individual or group being researched may not seem technically capable, they may have access to people who are, or may just be aided by the powerful algorithms employed by companies such as Google or Meta (formally Facebook) etc.

Any person undertaking III must consider the risk of their activity and think to themselves: “Am I okay with the person I am looking at knowing this information about me personally, or the investigation itself?” With this footprint in mind the NPCC has defined Internet Intelligence and Investigations areas of business as below.

3. Core Internet Use

3.1 The internet is now a fundamental part of everyday life it is recognised that all law enforcement employees should have access to the internet and in particular the World Wide Web (www). III is a core capability for all investigators involved in any form of investigation and touches on all threat areas.

Core Internet use is the overt and ad hoc use of online resources and search engines to provide basic information. Put simply; typing a query into a search engine such as google and reviewing the resultant returns is the essence of core internet use. This includes, but is not limited to:

• Capturing online evidence highlighted by a victim or witness.

• Accessing online mapping facilities in preparation for executive action.

• Utilising online data sources such as 192.com, Companies House, Local Government Planning Departments etc.

• Reverse image searching, exchangeable image file format (exif) data recovery, source code capture and review.

Under ‘Core Internet Use’ individuals will not access areas of the internet which require a username or password, unless accessing an authorised site using official log in details.

3.2 Equipment:

Core Internet use can be conducted from any networked computer or Mobile Data Terminal (MDT). Core Internet use must not be completed on non-attributable machines that have been set aside for Covert III activity. Personal social media profiles are not permitted for use for any form of internet research as this may lead to your identity and personal account details being made visible to the subject.

There are several browsers available to Surrey Police and Sussex Police employees including, Microsoft Edge, and Google Chrome. It is recommended that (redacted text) is used for Core internet use owing to the enabled extensions / add-ons which enable screen and video capture along with tools for reverse image searching and exif data review etc. (See DISU - Home) for more details on how to use these extensions effectively).

3.3 Training:

Core internet use is fundamental to our everyday lives so it is not expected that any additional training will be required. For staff wishing to enhance their capabilities or develop on a pathway towards the activity covered in subsequent sections it is recommended that staff undertake all Digital Learning and mandated packages on College Learn. These currently include Digital Policing Foundation Level 1, Digital Policing (all staff) and Operation Modify. There is further training available to all employees through the NCDS Academy which hosts an online open source course. Additionally, the DISU provide training material for above aspects of core internet searching which is accessible through their local SharePoint site.

3.4 Online Facial Recognition (OFR) tools.

Non-exhaustive examples of such OFR tools include Clearview AI, PimEyes, Amazon Rekognition, systems powered by Google, Microsoft, or Facebook.

The examples are provided to promote awareness of the types of OFR tools this policy covers. The examples listed do not reflect that any are or would be approved for use. Any consideration for use would need to be undertaken in line with this policy, and in some cases the nature of the online tool presents a high, if not insurmountable bar to lawful use. The process outlined in this policy allows such a determination to be made in line with the applicable legal framework.

This policy does not extend to:-

a) manually instigated facial recognition for retrospective searching of video / still images; or

b) human initiated facial search submitted from a mobile device in near real-time (known as officer initiated facial recognition); or

c) any use of offline third-party OFR systems, or data sharing for the purpose of facilitating the use of those systems; or

d) use of Live Facial Recognition (LFR).

The use of online FR tools may be an investigative tactic to help officers make identifications and progress investigations where Surrey Police or Sussex Police would otherwise struggle to do so. They generally work by analysing key facial features to generate a mathematical representation. This representation is then compared against faces held on the online tool's database to identify possible matches against a probe image. It is for Surrey and Sussex personnel to then make an identification. Any online FR tool will only suggest potential matches for consideration, and where appropriate, further investigation by Surrey and Sussex personnel. OFR search results are not evidential and will only be used in conjunction with additional identity procedures, this being human review to compare the images before any actions are taken by the police.

The probe images will only be searched where there is a defined policing purposes as defined in Part 3 of the Data Protection Act 2018, 'for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security' to be read in conjunction with UK General Data Protection Regulation (UK GDPR).

The use of an online OFR tool will typically be deployed only when less intrusive methods have been pursued or are deemed likely to fail. This would ordinarily and routinely include first checking facial recognition via the Police National Database (see the respective Force policy Use of the Police National Database (PND)).

Probe images must be lawfully held by Surrey Police or Sussex Police and consideration should be given to the availability of the probe image prior to utilising OFR tools.

Images already in wide circulation such as those circulated as 'identity sought' by social media appeals or images that have been captured from online sources will already be visible to online OFR tools.

Probe images that have limited circulation such as have been obtained directly by Surrey Police or Sussex Police e.g. from surveillance or body worn video (BWV) etc. should not be routinely searched using online OFR and authority must be provided by a DISU supervisor for online OFR tools to be used in these circumstances (see section 5 for further information).

3.5 Capturing Indecent Images of Children (IIOC) or other illegal Material from the internet or darknet.

This section should be read in conjunction with

Surrey: Policy and Practice for Viewing and Grading Indecent Images of Children (IIOC) or other Illegal Material

Sussex: Viewing Digital Material of an Indecent Nature Policy (1169)

Online Child Sexual Abuse and Exploitation (CSAE) can take several different forms which include:

Indecent Images of Children (IIOC) which are images of, or depicting, a child or part of a child which are judged to be in breach of recognised standards of propriety. Examples of images considered to be indecent are those depicting a child engaging in sexual activity or in a sexual manner, through posing, actions, clothing etc. IIOC includes photographs, videos, pseudo-photographs, and tracings.

Prohibited Images of Children are non-photographic images, for example Computer-generated imagery (CGI), cartoons etc, which portray a child engaging in sexual activity, a sexual act being performed in the presence of a child or focus on the child's genital or anal region. For full versions of relevant legislation please visit www.legislation.gov.uk.

Increasingly children are sharing unclothed or partially unclothed (colloquially referred to as 'nudes') with one another and strangers online. Some of this material will constitute IIOC and increasingly these images are being weaponised by blackmailers under 'sextortion' cases where images obtained under false pretences are then shared to friends and family. (See useful online guide to dealing with sextortion).

Where an open-source practitioner has been directed to suspected IIOC material online or has happened upon such material during the course of their policing activity there will often be a need to capture that information for evidential and/or safeguarding purposes. With amnesiac applications, disappearing posts / messages and the volatility of online material there will often be a need to capture material before it disappears. Social media networks have various measures in place to detect and take down IIOC material, but moderation and compliance capability differs across the various platforms and therefore on occasion police staff will see or be directed to material even on mainstream platforms on the clear web.

Determining whether material meets the definition of IIOC can only be conducted by individuals who have completed the National Accredited Grading (NAG) training programme. Typically, such staff are employed in Paedophile Online Investigation Team (POLIT) (Surrey), Online Child Abuse Team (OCAT) (Sussex) and Digital Forensic Team (DFT), guidance should be sought from a trained individual in determining whether found material is in fact to be considered IIOC at which stage the following process can be followed. Where a trained grading officer is not available and there is a risk of loss of evidence by failing to capture the material there and then the following guidance will be taken using an abundance of caution in determining whether the material is 'likely' to meet the definition.

Where online practitioners need to capture suspected IIOC material great care must be taken to do this in a considered manner minimising the further copying, exposure, and dissemination of the material. (See link to Crown Prosecution Service (CPS) memorandum of understanding for more details and context here: Memorandum of Understanding Between the Crown Prosecution Service (CPS) and the National Police

Chiefs' Council (NPCC) concerning Section 46 Sexual Offences Act 2003 | The Crown Prosecution Service)

Devices that are not connected to the police network such as standalone laptops and covert mobile devices should be used for this purpose and where available staff in the DISU or Sussex OCAT are to be utilised. A supervisor of one of these departments must be made aware of the existence of potential IIOC material being captured. In Sussex OCAT would be the first preference specifically utilising the services of the OCAT Referral Unit in Surrey DISU will take primacy.

The process for capturing online material (NOT cloud acquisition / account takeovers etc.) is as follows:

Mobile Phone: Where a mobile phone has been utilised the capture path of any downloader or screen capture tool should be altered to capture material DIRECTLY to external encrypted USB or password protected hard drives where this is not possible due to restrictions in the ability to direct saved captures then internal removable storage such as micro SD cards should be used. When the required material has been captured the storage device should be removed from the mobile phone and placed in a sealed police evidence bag clearly denoted to contain possible IIOC.

Where a laptop or desktop device is used for capture, the same process will be adopted using either removable encrypted USB or password protected removable storage in place of a micro SD.

Surrey Process:

In Surrey the sealed exhibit is to be taken to Surrey POLIT. Where this is not possible the same day then the departmental supervisor who manages the capturing practitioner will direct how the material is to be securely stored until it can be taken to the above departments.

When Surrey POLIT have taken possession of the storage of the exhibit the contents will be transferred to their long-term electronic storage and the removable storage device will be forensically wiped prior to it being reused. POLIT staff will grade the material and provide guidance on the processes to identify victims should this be required. POLIT will not necessarily adopt investigative responsibility, and this should be decided when transferring the material. A record of the above will be recorded and preserved for continuity purposes to describe the above transfer of material.

Where a crime / safeguarding incident has not yet been recorded and the material is discovered whilst undertaking other duties, it will be the responsibility of the requesting department who asked for the open source research to further investigate and appropriately record any criminal offences, after conversing with POLIT.

Sussex Process:

In Sussex the sealed exhibit is to be booked into the evidential property Store through Niche and clearly marked as potentially containing IIOC or by agreement taken to one of the operational OCAT offices and booked into their localised storage.

Where this is not possible the same day then the departmental supervisor who manages the capturing practitioner will direct how the material is to be securely stored until it can be taken to the above departments.

Sussex OCAT will then be consulted as to how the material is to be graded and whether there are any victim identification requirements. OCAT will not necessarily adopt investigative responsibility, and this should be discussed when transferring the material. A record of the above will be recorded and preserved for continuity purposes to describe the above transfer of material.

Where a crime / safeguarding incident has not yet been recorded and the material is discovered whilst undertaking other duties, it will be the responsibility of the requesting department who asked for the open source research to further investigate and appropriately record any criminal offences, after conversing with OCAT.

Removal of online material

Images and material should not be left online once appropriate captures have been obtained and evidence secured. The process and ease in which individual platforms can be notified that IIOC of other illegal material on their platforms differs between organisations.

Sexual images or videos of someone who could be under 18 online can be easily reported by any person to the Internet Watch Foundation (https://report.iwf.org.uk/en).

Police employees wanting to report relevant material online should in the first instance raise it to their supervisor. Contact should then be made with POLIT / OCAT as to how to proceed.

4. Internet Investigations (Overt)

4.1 'Internet Investigations (Overt)' is a structured, methodical, task driven planned approach to online investigations and research, conducted by suitably trained (see below) individuals. Often overt investigations will start with aspects of core internet use but under this section searching the internet is not intended to be ad-hoc or minimal but instead is a more focussed and determined attempt to obtain information to meet the needs of an investigation by researching the internet. Activities which fall into this capability descriptor include but are not limited to:

• Accessing areas of the internet which require a username or password; (see caveats below)

• Utilising advanced search techniques to conduct systematic and focussed research;

• Reviewing online activity in relation to pre-planned and spontaneous events;

• Capturing intelligence and/or evidence in support of an ongoing investigation;

• This policy does not cover overt engagement with witnesses and victims over social media.

4.2 All activity online should be overt, with a view of trying to ensure that the activity is seen overtly.

It is recognised that the preceding statement of purpose has caused significant confusion and frustration by employees historically trying to conduct overt internet investigations. Previous iterations of this policy have subsequently described how ‘overt profiles’ should be set up on social media platforms to conduct internet investigations, detailing that these accounts should be set up by corporate communications and contain details identifying the account as being owned by the police.

Extensive research by the DISU and other law enforcement teams have found that setting up overt accounts on Meta and other major social media platforms has quickly led to the accounts being suspended or shut down by the platforms. It is impossible to determine exactly why these accounts are being flagged as suspicious by the platforms, but testing indicates it is likely to include the wording used, use of police crests and access via law enforcement internet access (through attributable Police Internet Protocol (IP) addresses).

Since ‘standalone’ or other methods of obfuscating IP addresses are not currently available outside specialist teams, overt internet investigations remain limited. At present, this means overt investigations involving social media platforms will effectively be limited to the research, review, and capture of information from social media sites that do not require a specific login or only require limited details such as Youtube, WhatsApp (available on MDT) etc.

Accessing sites such as SnapChat, Facebook, Instagram, X (formally known as Twitter), Telegram, Kik, etc. from police attributable accounts / devices is not advised and instead should be tasked to those trained to conduct covert internet investigations (see below).

4.3 Where information is required from social media platforms that require a username and password to access the online space then it is accepted that a covert profile will be used owing to the enforced limitations detailed above. Any requests should be tasked to a relevant team empowered to conduct covert internet investigations such as within intelligence units. The practitioners conducting such tasks should use profiles specifically set aside for overt investigations which should contain only the minimal information for creation and survival. The practitioner should specifically record that the research and any screen or video captures have been conducted as part of an overt investigation.

In practice overt investigations involving access to accounts that require a profile and login such as some social media sites will typically be in response to information suggesting information is present that requires capture to evidence criminality. Such examples may be where police are directed to a social media platform where a video of an assault has been uploaded or where comments have been made that identify an offender or are in themselves considered a criminal offence such as material posted which constitutes offence under the Malicious Communications Act 1988 or other such legislation. In addition, such activity will be restricted to capturing the information and NOT continuing to monitor the account for further activity.

4.4 No Activity requiring authorisation under Regulation of Investigatory Powers Act 2000 (RIPA) or other covert authority, will be conducted under this section. It should be noted that the ‘systematic or persistent monitoring’ of a personal profile, even where the profile

is open, will be considered directed surveillance, if it is not clear to the subject that such activity is taking place. Due to the requirement for Regulation of Investigatory Powers Act 2000 (RIPA) authorisation for this activity falls within Covert Internet Intelligence and Investigations. This will include the persistent monitoring of groups in relation to pre-planned and spontaneous events / protests where personal information is sought or gained.

4.5 Systematic monitoring of news / public channels where there is no expectation of privacy and an expectation of law enforcement presence may be conducted under this section without authority, examples may include neighbourhood watch groups where information is specifically shared with the purpose of police assistance or monitoring channels to determine numbers of individuals likely to attend an event.

4.6 It should be noted that the need to conduct overt internet investigation will often be negated in favour of capturing best evidence from source. For example, where a member of the public reports to the police that they have seen posts on the internet that suggest a crime has happened, and an overt policing response is required then they should be asked to capture that digital evidence themselves. Additionally where posts are made within victim or witnesses accounts or direct messages sent to them the victim / witness can request copies of their account information directly from the platforms which can then be made available to the police (the following website explains how users can get copies of their own data https://justgetmydata.com/).

4.7 Equipment:

• Activity under this descriptor can be completed via the web browser on any networked computer without the need to use a covert profile.

• Various types of capture software are available through programs such as Google Chrome or Microsoft Steps (see DISU SharePoint for guides on how to use capturing tools)

• No Overt III activity will be conducted on police employees' personal devices or on any device where the resulting footprint may lead to an individual working for, or acting on behalf of, the police being placed at unmitigated risk. Personal social media profiles are not permitted for use;

• Where covert profiles are required for overt investigations then IP obfuscation equipment or software may be used but, as stated separate profiles should be put aside for overt investigations.

4.8 Training:

Any person involved in this activity descriptor must have as a minimum:

• Completed Digital Policing Foundation Level 1, Digital Policing (all staff) and Operation Modify;

• Completed the III module on NCDS Academy;

• Completed the Surrey / Sussex IDP Digital Policing Course (or equivalent).

4.9 Missing Persons (Sussex only). The missing persons units in Sussex Police do operate OVERT profiles principally used to contact missing persons on social media. For information refer to Missing Person Policy (558). These processes are not discussed in this document.

5. Internet Investigations (Covert)

5.1 Covert III is a structured, methodical, task driven planned approach to covert online research, conducted by a suitably trained (and current) individual. When authorised, activities which fall into this descriptor include but are not limited to:

• (Redacted text);

• Covertly gather evidence and intelligence;

• Conduct online surveillance of a known subject or group;

• Facilitate the deployment of additional online covert tactics;

• Routine use of III covert profiles.

A III Covert Profile is defined as a profile designed or created to obfuscate the fact it is being used for a policing purpose. The nature of an III Covert Account can range significantly from a simple anonymised username which is obvious fictitious, such John Doe etc. to a full covert legend. It also important to note that III Covert Profiles can portray people, businesses, groups etc. Creation of covert profiles should follow the guidance provided in 10.2 NPCC III Covert Profile Guidance and the processes described will not be repeated here.

5.2 Systematic or persistent monitoring of a personal profile is directed surveillance if it is not clear to the subject or group that such activity is taking place. Covert III tactics will only be utilised after all other reasonable, less intrusive, methods have been considered and it is proportionate and justified to do so. Often practitioners will conduct covert activity as a precursor to directed surveillance. Historically this has been colloquially described as ‘scoping’ or ‘initial research’ or only accessing a subjects social media account ‘once’ before Directed Surveillance Authority (DSA) is considered, unfortunately, in practice this is not that simple. The surveillance codes of practice (section 3) provide specific guidance for online surveillance, and these should be read in full when making a determination of whether DSA is required - elements of this information have been extracted here to assist our understanding.

Simple reconnaissance of sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person’s reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording private information about a particular person or group, a directed surveillance authorisation should be considered. The pluralisation of ‘collect’ and ‘record’ again suggests that DSA authority is more likely to be required when practitioners are repeatedly viewing information relating to the same individual.

The codes further state that the study of an individual’s online presence becomes persistent, or where material obtained from any check is to be extracted and recorded

and may engage privacy considerations, RIPA authorisations may need to be considered.

5.3 Covert III will often require a DSA, or other covert authority, to be considered. If there is doubt by the practitioner whether a DSA is required, then advice should be sought from a supervisor or RIPCOM and rationale for any decision making can be appropriately recorded. In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website or social media site as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

• Whether the investigation or research is directed towards an individual or organisation;

• Whether it is likely to result in obtaining private information about a person or group of people;

• Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

• Whether the information obtained will be recorded and retained;

• Whether the information is likely to provide an observer with a pattern of lifestyle;

• Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

• Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

• Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

Therefore, all practitioners who conduct Covert Internet Investigations must be familiar with the content of the following;

Regulation of Investigatory Powers Act 2000 (RIPA)

Covert Surveillance and Property Interference – Revised Codes of practice 2018 (See specifically section 3.10 to 3.17 'Online Surveillance')

Covert Human Intelligence Sources (CHIS) draft revised code of practice December 2021 (See specifically sections 4.26 to 4.32 'Online Covert Activity)

Both codes of practice, mentioned above, contain specific guidance in relation to online activity, however the documents must read, and guidance applied in full. It can be helpful to view RIPA as a tool to provide protection to the practitioner, rather than an instrument that provides permission. The key points for any practitioner to consider in relation to the application of authorities – What am I doing and why and I doing it?

The initial research of social media to identify a potential threat, establish facts, confirm the availability of goods or services; or corroborate an intelligence picture is unlikely to

require an authorisation for directed surveillance, whereas repeated visits, building up a profile of a person's lifestyle or the nature of a group's activities would do so.

Each case must be considered on its individual circumstances and early discussion between the investigator, RIPCOM and the Authorising Officer is advised to determine whether activity should be conducted with or without the protection of an authorisation. If the aim is to gather evidence / intelligence against specific individuals from the outset, then it may be appropriate to have a DSA before any activity is commenced.

5.4 Covert III activities will only be conducted by personnel who are suitably trained (and current) must have viewed the DSA prior to conducting any online activity.

5.5 (Redacted text)

5.6 Any electronic data that needs to be transferred to a police system must be transferred using an approved method (i.e. encrypted and force accepted USB storage device) and this hardware must be checked for malware or malicious software prior to entry to the police system (i.e. scanned with 2 separate antivirus on non-attributable device).

5.7 Auditing the activity undertaken must be completed to show the route that was taken on the internet and the result. This must be recorded so that a person following the process could recreate the route if necessary. If unlikely that the route would remain the same screen capture software will also aid this process.

5.8 Maintaining the covert aspect of online activity can be complex and involves a wide range of tactics and processes being employed to minimise the risk of compromise. Practitioners must be satisfied that the effort taken to maintain the covert nature of their activity meets the level necessary for the individual task, and associated risk of compromise. Measures taken to ensure the covert nature of the activity is not compromised, must be assessed against the subject's capability or Organised Crime Groups (OCG) potential capability, the nature of the crime or event being investigated and the impact of inadvertent compromise.

5.9 (Redacted text)

Since DSA activity concerns itself with obtaining private information simple reconnaissance of social media groups (redacted text) to identify whether they are of legitimate police interest is initially unlikely to require an authorisation for directed surveillance. Repeated visits, building up a profile of a person's lifestyle or the nature of a group's activities would require a standalone directed surveillance authority. (redacted text) Officers and staff should seek RIPCOM advice if in doubt.

(Redacted text)

Practitioners should not instigate any conversations with users of other accounts, regardless of whether they are the subject of the investigation without a use and conduct authority and suitable training. (Redacted text)

5.10 Equipment:

• (Redacted text)

• Encrypted removable media must be available for storage and transfer of any material as necessary.

5.11 Training:

• Completed Digital Policing Foundation Level 1, Digital Policing Foundation Level 2 and Operation Modify;

• Completed the III module on NCDS Academy;

• There are several training courses designed to teach covert III and any one of the following are considered highly desirable for practitioners routinely conducting covert III;

• CoP National Policing Curriculum Learning standards for Internet, Intelligence and Investigations: Covert Investigator (Formally RITES course);

• SORINTEQ intermediate i3 investigators course;

• VESTIGO III-Pro course.

5.12 (Redacted text)

5.13 Dark Web

Dark Web (non-indexed web)

The dark web is web content that exists on darknets: where users need specific software to gain access to the content. Users can remain completely anonymous whilst browsing the dark web, and it can be used for a multitude of reasons:

• Visit dark web markets and purchase drugs, firearms, weapons, computer malware etc.

• Communicate securely with others without metadata or content surveillance.

• Access free media e.g., BBC News in countries that have oppressive regimes.

The dark web is accessed mostly through TOR (The Onion Router), which is a free and easily accessible browser that allows users to navigate to the clearnet (normal web browsing) and dark net simultaneously.

There is also an alternative service to TOR through I2P (The Invisible Internet Protocol). I2P runs on a peer-to-peer network of computers worldwide and each user runs the I2P router on their computer and provides encrypted one-way connections to and from other users. No one can see what the traffic is, where it is going or where it has come from. I2P uses garlic routing – which divides your message into smaller messages, called cloves, and they are then encrypted and sent out separately across the network until they reach their destinations.

A large amount of criminality can be conducted on the dark web, including (but not limited to):

• Drug supply and importation.

• Purchase of firearms.

• Indecent images of children.

• Hacking, doxing, DDOS attacks for hire etc.

• Purchase of stolen credit card, PayPal and other financial data.

• Purchasing fraudulent documents – e.g., passports, visas etc.

It is estimated there are over 65,000 .onion address links and believed to be over thirty million TOR users. This number appears to be growing, surpassing three million users a day by mid-2022.

Any open source deployments on the dark web by Surrey Police or Sussex Police law enforcement should be conducted by capable and competent staff. The DISU III practitioners are trained to operate in this space and enquiries requiring access to the dark web should be tasked through the DISU using the standard tasking process.

The DISU will ensure that appropriate deconfliction with regions specialist teams is conducted and will also provide a feasibility assessment as to the viability of the tasking.

To determine feasibility of any taskings to capture intelligence / information on the dark web DISU need actionable intelligence / information. Suggestions that, (redacted text) will almost always be insufficient without further information and render meaningful deployments extremely difficult if not practically impossible to action as a practitioner. The main pieces of information needed to effectively scope the dark web are:

(Redacted text)

(Redacted text)

(Redacted text)

6. Welfare

6.1 Anyone practising open source research within their job role, runs the risk of viewing distressing content online. A separate guidance document has been produced to help those exposed to distressing content which is available III Exposure to Distressing Content.

The purpose of this guidance is to Prevent, Prepare and Act on the effects that open source intelligence (OSINT) research may have on the practitioner and supply the tools to help them through every step of the process. Sometimes the impact to the practitioner from prolonged exposure to unpleasant material will not be immediately recognised, this is especially the case with cumulative impacts which are not as obvious as they unfold.

Distressing content is often assumed to consist solely of extreme imagery or videos, such as Child Sexual Abuse Material (CSAM) or acts of severe violence found in the darker corners of the internet. However, distressing content encompasses a much broader range of material, and what may be upsetting can vary greatly between individuals and even from one day to the next. While much of the guidance document offers practical advice for individual actions, managers and organisations also have a duty of care to provide support. Open and candid discussions between practitioners and their supervisors are encouraged to communicate how exposure to such content is affecting well-being and to explore supportive measures for the short, medium, and long term.

Team: Specialist Crime Command